IN THE CLAIMS

Please amend the claims as follows:

Claim 1-14 (Canceled).

Claim 15 (New): A system for protecting a communication device against a denial-of-service attack, the system comprising:

a monitoring device configured to be provided on a local area network to which the communication device that is a target of the denial-of-service attack is connected, the monitoring device monitoring a packet transmitted to the communication device via an internet-service-provider network; and

a restricting device configured to be provided on the internet-service-provider network, the restricting device restricting a packet to the local area network, wherein

the monitoring device includes

an attack detecting unit that detects an attack by the packet on the communication device, and

a protection-request-information transmitting unit that transmits protection request information indicating a request for protection against the attack to the restricting device; and

the restricting device includes a packet restricting unit that restricts a packet transmitted to the communication device via the internet-service-provider network based on the protection request information.

Claim 16 (New): The system according to claim 15, wherein

the monitoring device further includes a signature generating unit that generates a signature indicating a feature of a packet that attacks the communication device,

the protection-request-information transmitting unit transmits the protection request information including the signature to the restricting device, and

the packet restricting unit restricts a packet corresponding to the signature.

Claim 17 (New): The system according to claim 16, wherein

the restricting device further includes a signature determining unit that determines whether the protection request information including the signature is appropriate, and

the packet restricting unit restricts a packet corresponding to a signature that is determined to be appropriate, and does not restrict a packet corresponding to a signature that is determined to be inappropriate.

Claim 18 (New): The system according to claim 16, wherein

the restricting device further includes

a report generating unit that generates a report on a feature and an amount of a packet corresponding to the signature, and

a report transmitting unit that transmits the report to the monitoring device;

the signature generating unit generates a new signature based on the report,

the protection-request-information transmitting unit transmits the protection request information including the new signature to the restricting device, and

the packet restricting unit restricts a packet corresponding to the new signature.

Claim 19 (New): The system according to claim 18, wherein

the restricting device further includes a forwarding unit that forwards the protection request information to other restricting device provided on the internet-service-provider network, and

the forwarding unit determines whether to forward the protection request information based on the report generated by the report generating unit, and forwards the protection request information to the other restricting device upon determining that it is necessary to forward the protection request information.

Claim 20 (New): The system according to claim 17, wherein

the restricting device further includes a determination-result transmitting unit that transmits a result of determination of the signature determining unit to the monitoring device, and

when the result of determination indicates that the signature is inappropriate, the signature generating unit generates, based on the result of determination, a new signature indicating the feature of the packet that attacks the communication device.

Claim 21 (New): A method of protecting a communication device against a denial-of-service attack using a monitoring device and a restricting device, the monitoring device being configured to be provided on a local area network to which the communication device that is a target of the denial-of-service attack is connected and monitoring a packet transmitted to the communication device via an internet-service-provider network, the restricting device being configured to be provided on the internet-service-provider network and restricting a packet to the local area network, the method comprising:

attack detecting including the monitoring device detecting an attack by the packet on the communication device;

protection-request-information transmitting including the monitoring device transmitting protection request information indicating a request for protection against the attack to the restricting device; and

packet restricting including the restricting device restricting a packet transmitted to the communication device via the internet-service-provider network based on the protection request information.

Claim 22 (New): The method according to claim 21, further comprising:

signature generating including the monitoring device generating a signature indicating a feature of a packet that attacks the communication device, wherein

the protection-request-information transmitting includes transmitting the protection request information including the signature to the restricting device, and

the packet restricting includes restricting a packet corresponding to the signature.

Claim 23 (New): The method according to claim 22, further comprising:

signature determining including the restricting device determining whether the protection request information including the signature is appropriate, wherein

the packet restricting includes

restricting a packet corresponding to a signature that is determined to be appropriate; and

not restricting a packet corresponding to a signature that is determined to be inappropriate.

Claim 24 (New): The method according to claim 22, further comprising:

report generating including the restricting device generating a report on a feature and an amount of a packet corresponding to the signature; and

report transmitting including the restricting device transmitting the report to the monitoring device, wherein

the signature generating includes generating a new signature based on the report,

the protection-request-information transmitting includes transmitting the protection request information including the new signature to the restricting device, and

the packet restricting includes restricting a packet corresponding to the new signature.

Claim 25 (New): A computer-readable recording medium that stores a computer program for protecting a communication device against a denial-of-service attack using a monitoring device and a restricting device, the monitoring device being configured to be provided on a local area network to which the communication device that is a target of the denial-of-service attack is connected and monitoring a packet transmitted to the communication device via an internet-service-provider network, the restricting device being configured to be provided on the internet-service-provider network and restricting a packet to the local area network, wherein

the computer program causes a computer to execute:

attack detecting including the monitoring device detecting an attack by the packet on the communication device;

protection-request-information transmitting including the monitoring device transmitting protection request information indicating a request for protection against the attack to the restricting device; and

packet restricting including the restricting device restricting a packet transmitted to the communication device via the internet-service-provider network based on the protection request information.

Claim 26 (New): The computer-readable recording medium according to claim 25, wherein

the computer program further causes the computer to execute signature generating including the monitoring device generating a signature indicating a feature of a packet that attacks the communication device,

the protection-request-information transmitting includes transmitting the protection request information including the signature to the restricting device, and

the packet restricting includes restricting a packet corresponding to the signature.

Claim 27 (New): The computer-readable recording medium according to claim 26, wherein

the computer program further causes the computer to execute a signature determining procedure of determining including the restricting device determining whether the protection request information including the signature is appropriate,

the packet restricting includes

restricting a packet corresponding to a signature that is determined to be appropriate by the signature determining unit, which is to be transmitted to the communication device; and

not restricting a packet corresponding to a signature that is determined to be inappropriate, which is to be transmitted to the communication device.

Claim 28 (New): The computer-readable recording medium according to claim 26, wherein

the computer program further causes the computer to execute:

a report generating procedure of generating including the restricting device generating a report on a feature and an amount of a packet corresponding to the signature; and

a report transmitting procedure of transmitting including the restricting device transmitting the report to the monitoring device,

the signature generating procedure includes generating a new signature based on the report,

the protection-request-information transmitting procedure includes transmitting the protection request information including the new signature to the restricting device, and

the packet restricting procedure includes restricting a packet corresponding to the new signature, which is to be transmitted to the communication device.